

AD-HOC RADIO COMMUNICATION VERIFICATION SYSTEM

Field of the Invention

The present invention relates to an ad-hoc radio communication verification system, ad-hoc radio communication data send/receive system, ad-hoc radio communication verification method, ad-hoc radio communication data send/receive method for coping with tampering of transmission data, and further a recording medium and delivery apparatus for recording and delivering a corresponding program, respectively.

Background

In order for two unspecified parties to transmit data without having the data tampered with by a malicious third party in an ad-hoc short-haul radio communication such as ad-hoc radio communication that does not utilize a specific infrastructure, it is necessary to share a cipher key that is unknown to the malicious third party. However, a method for properly setting a value behind the cipher key during communication is complicated, therefore, particularly under the circumstance where communicating parties meet for the first time, it is impractical that they exchange the cipher key by parol or memo writing. One method for automatically sharing a cipher key is to share a public key first and then encrypt the cipher key using that public key to share.

However, there is a risk of Man-in-the-middle attack (For

details on Man-in-the-middle attack, refer to the publication titled "APPLIED CRYPTOGRAPHY", John Wiley & Sons, Inc., pages 48-50, by Bruce Schneier).

Now the risk of data tampering in the Man-in-the-middle attack will be summarized. Fig. 1 shows that a malicious third party C intervenes between a source A and a destination B in an ad-hoc radio communication system 10, without both parties noticing this intervention. Despite parties A and B believe that a communication path is established between them directly as shown in Fig. 1(a), practically the third party may intervene between them as shown in Fig. 1(b). Now it will be described how the Man-in-the-middle attack is performed by way of a concrete example.

A common procedure for establishing a radio cipher communication path is as follows.

Procedure 1: The source makes a call to an unspecified number of parties using an ID of the destination it desires to communicate with.

Procedure 2: If the destination is located within the coverage area, it receives the ID (i.e., own ID).

Procedure 3: The destination communicates its operating conditions or the like to the source.

Procedure 4: Both parties determine the operating parameters together necessary for establishing a communication path (e.g., selection and setting of a communication path to be used, exchange of a cipher

key, etc.).

Procedure 5: The communication path is established and mutual communication starts.

5 The timing when the malicious third party is most liable to intervene at the position C shown in Fig. 1 is the timing when both parties subject to wiretapping begin the radio communication face to face. That is, the intervention may occur during above listed procedures 1 - 3. Fig. 2 and Fig. 3 shows an example of methodology for a malicious third
10 party to intervene at the position C shown in Fig. 1. According to the nature of the radio wave, the source A is forced to make a call to all surrounding destination candidates using a specific ID (procedure 1). The destination B listens for a call of its own ID (procedure
15 2), and responds to source A (procedure 3). At this moment, a malicious third party tries to make a pretense as mentioned below, by responding to a call to an ID other than its own or making a call using an ID other than its own. First of all, the malicious third party sends out a noise of
20 the same frequency band against a response from destination B and hinders source A from listening for that response. At this moment, destination B does not know the fact of noise, so that it goes on to the procedure 4 and waits for the start of sessions from source A in the procedure 4. Since
25 source A is not in the procedure 4, destination B returns to a condition again where it listens for a call of its own ID after the time-out. On the other hand, source A does not get a response from destination B, thus it usually makes a

call using the same ID after the time-out (procedure 1).
That is, source A and destination B try to synchronize the
procedure each other, then they become aware of the failure
by the time-out, then they return to the original
5 conditions.

The malicious third party waits in tune with the timing when
source A makes a call again using the same ID, and further
waits in tune with the timing when destination B again
starts listening for the call of its own ID. Thereafter,
10 the malicious third party C responds to the call from source
A by pretending destination B, and makes a call to
destination B that starts listening for a call of its own ID
by pretending source A. Of course, the malicious third
party has a capability to change its own ID to any ID. The
15 reason why the malicious third party can make such two
pretense behavior is that the timing is not the same when
source A and destination B return to the original conditions
due to out of synchronization of the mutual procedure. This
results from the fact that the timing when source A and
20 destination B start waiting for a next event is originally
different and that an event subject to the time-out is also
different, hence the time-out period itself is different.

Due to this pretense maneuver, source A believes that it
received a normal response from a proper destination B and
25 proceeds with the malicious third party C on and after the
procedure for establishing the communication path, i.e.,
procedure 4, while destination B believes that it received a

call from a proper source A and proceeds with the malicious third party C as well. When proceeding to the procedure 5, the malicious third party can wiretap by relaying communication data between both parties, without coming to a knowledge of both parties A and B who want to secure the communication path by themselves. Utilizing this pretense (i.e., relay), a public key that source A is to send to destination B can be tampered with by the third party C and changed with a public key corresponding to a private key that the third party C prepared in advance. As a result, a cipher communication path that is essentially constructed between source A and destination B is only effective between source A and the third party C, while another communication path is established between the third party C and destination B by the third party C. That is, encrypted data sent from source A is decoded by the third party C, then it is transmitted over a cipher communication path between the third party C and destination B, with applying another encryption. The same applies to the reverse transmission. Despite both source A and destination B establish the cipher communication path in a normal procedure, they are changed their public key without knowing it, consequently wiretapped. Such an attack (i.e., wiretapping by pretense) is called Man-in-the-middle attack. Since the cipher communication path itself is safe, it is essential that both parties who communicate truly share the same public key, as a countermeasure against such an attack.

[Problems to be Solved by the Invention]

As a countermeasure against the Man-in-the-middle attack, it is conceivable to display a personal ID (typically the name of an opponent) described in a certificate on the sending side and destination side to compare, using the certificate issued by a certification body. However, it costs to issue the certificate. Also, when utilizing a certification body, it is necessary to register one's identity for authentication, thus resulting in publishing own identity to an opponent, whereby anonymity can not be kept. Further, when utilizing a service such as Yellow Page that specifies a user from a public key, there is needed a secure network connection based on the phone line, for example, which costs for transaction.

Summary of the Invention

Therefore, it is an aspect of the present invention to provide an ad-hoc radio communication verification system, ad-hoc radio communication data send/receive system, ad-hoc radio communication verification method, ad-hoc radio communication data send/receive method for effectively preventing tampering of data due to the pretense of a communication opponent, when sending and receiving data between the data sending and receiving devices that are mutually connected by an ad-hoc radio connection, and further a recording medium and delivery apparatus for recording and delivering a corresponding program, respectively.

It is another aspect of the invention to provide an ad-hoc radio communication verification system, ad-hoc radio communication data send/receive system, ad-hoc radio communication verification method, ad-hoc radio communication data send/receive method for verifying a communication opponent efficiently and smoothly, without exchange of passwords by parol or memo writing and without utilizing a certification body that publishes one's identity, and further a recording medium and delivery apparatus for recording and delivering a corresponding program, respectively.

Brief Description of the Drawings

These and other aspects, features, and advantages of the present invention will become apparent upon further consideration of the following detailed description of the invention when read in conjunction with the following drawing figures:

Fig. 1 shows that a malicious third party C intervenes between a source A and a destination B, without both parties noticing this intervention.

Fig. 2 shows the first part of an example of methodology for a malicious third party to intervene at the position C shown in Fig. 1.

Fig. 3 shows the second part of an example of methodology for a malicious third party to intervene at the position C shown in Fig. 1.

Fig. 4 is a flowchart illustrating the verification of data integrity and subsequent cipher data transmission.

Fig. 5 is a histogram showing an example of verification data generated from data for verification data generation.

Fig. 6 shows the first method to generate verification data from data for verification data generation using a one-way function.

Fig. 7 shows the second method to generate verification data from data for verification data generation using a one-way function.

Fig. 8 shows the third method to generate verification data from data for verification data generation using a one-way function.

Fig. 9 is a block diagram showing a method for getting verification data by combining the processing of Fig. 6 to Fig. 8.

Fig. 10 is a block diagram of a data send/receive device 20.

Fig. 11 is a flowchart of communication processing on the side of source A.

Fig. 12 is a flowchart of communication processing on the side of destination B.

Fig. 13 is a diagram for illustrating how to establish a cipher communication path for an ad-hoc radio connection between users who utilize a hidden computing style.

Description of the Symbols

10: Ad-hoc radio communication system

80a, 80b: PDA (Personal information terminal having radio communication function)

5 88a, 88b: Notebook computer (Personal computer having radio communication function).

Description of the Invention

10 According to the present invention, there is provided an ad-hoc radio communication verification system and method, respectively comprising the means or the steps of: sending data for verification data generation from one data send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection; in the one data send/receive device, generating verification data from the sent data for verification data generation based on a first generation algorithm and outputting the generated verification data to its own verification data output section; in the other data send/receive device, means for generating verification data from the received data for verification data generation based on the first generation algorithm and outputting the generated verification data to its own verification data output section; and determining whether the verification data at the verification data output sections of both the

15

20

data send/receive devices matches mutually.

The distance between both the data send/receive devices is typically less than 10 m, preferably several meters, such that a user can come and go, since the verification data needs to be compared mutually at the verification data output sections of both the data send/receive devices. The verification data generated based on the data for verification data generation may be the data for verification data generation itself. The verification data is set such that it is easily determined whether the verification data at the verification data output section of both the send/receive devices matches mutually or not. Generally, if the verification software that is used in both the data send/receive devices is the same, the same generation algorithm is used to generate the verification data from the data for verification data generation. However, one of a plurality of generation algorithms may be determined at pleasure on the spot by both the data send/receive devices.

One data send/receive device generates verification data from the sent data for verification data generation based on the first generation algorithm. The other data send/receive device generates verification data from the received data for verification data generation based on the first generation algorithm. Then, it is determined whether the verification data output from the verification data output sections of both the data send/receive devices matches

mutually. If affirmative, it shows that the data for verification data generation is properly transmitted from one data send/receive device to the other data send/receive device without tampered with on the way, that is, data integrity has been verified. In this way, data integrity is efficiently verified.

According to the ad-hoc radio communication verification system and method of the present invention, the verification data is visual or auditory verification data.

The visual verification data includes an image, a numeric, a character, and a combination thereof. As an example of the visual display of verification data, when the verification data is total n bits of bit data, for example, n bits are divided into consecutive equal number of bits, then the histogram is created wherein the x-axis represents to the divisions, while the y-axis represents the quantity corresponding to each division. As an example of the auditory display of verification data, a sound with a pitch corresponding to each division of the aforementioned histogram is output in order from the lower division. The verification data should be selected such that a user can smoothly and correctly determine whether the verification data in both the data send/receive devices matches or not.

According to the ad-hoc radio communication verification system of the present invention, the verification data is output at the verification data output section both in the visual form and auditory form.

There may be a case where the difference of the verification data is apparent in the auditory output form in both the data send/receive devices, even if the visual output form of the verification data is similar, and vice versa. Accuracy of determination of match or mismatch is improved by comparing the verification data both in the visual output form and in the auditory output form.

The ad-hoc radio communication verification system and method of the present invention further comprise the means or steps of: defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the operator; establishing a serial sequence of operators that are composed of one or more of operators arranged in series, wherein the operators relate to the same or different one-way functions; and letting an input to the serial sequence of operators be the data for verification data generation and an output from the serial sequence of operators or a corresponding value be the verification data.

The one-way functions include a hash function, for example. The operators sequence defined above includes what includes only one operator. By associating a one-way function with the generation of verification data from the data for verification data generation, the difficulty for finding data for verification data generation from verification data increases, hence a likelihood decreases that a malicious

third party tampers with data using spurious data similar to true data for verification data generation. It is noted that finding the data for verification data generation from verification data becomes more difficult in terms of
5 calculated amount, when the length of the serial sequence of operators gets longer.

According to the ad-hoc radio communication verification system and method of the present invention, the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually.
10

The likelihood that all the plurality of verification data are similar is very low. Accuracy of verification improves by generating a plurality of verification data and determining for each of them whether the verification data matches mutually at the verification data output sections of both data send/receive devices.
15

The ad-hoc radio communication verification system and method of the present invention further comprise the means or steps of: defining a function as an operator, a numeric the operator operates on as an input of the operator, and an operation result of the operator as an output of the
20 operator; establishing a serial sequence of operators that are composed of two or more of operators arranged in series,
25

wherein the operators relate to the same or different one-way functions; letting an input to the serial sequence of operators be the data for verification data generation and outputs of two or more of operators selected from all operators composing the serial sequence of operators or corresponding values be the verification data respectively; and determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

The ad-hoc radio communication verification system and method of the present invention further comprise the means or steps of: defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the operator; establishing a plurality of operators that relate to mutually different one-way functions; letting the data for verification data generation be a common input to each operator and an output of each operator or a corresponding value be the verification data respectively; and determining for each verification data whether the verification data match mutually at the verification data output sections of both the data send/receive devices.

According to the ad-hoc radio communication verification system and method of the present invention, the data for verification data generation is a public key of either data send/receive device.

If the data for verification data generation is a public key

of one data send/receive device, the other data send/receive device can verify that the received public key is the public key of the one data send/receive device from the verification data. Therefore, the cipher communication
5 between both data send/receive devices is established completely using a symmetric key, for example, by sending the symmetric key from the other data send/receive device to the one send/receive device by the cipher communication using the public key of the one data send/receive device.

10 According to an ad-hoc radio communication data send/receive system and method of the present invention utilizing the aforementioned ad-hoc radio communication verification system, the system includes a portable terminal having a radio communication function and a personal computer having
15 a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the ad-hoc radio communication verification system verifies that a public key K_p of one user is transmitted from the portable terminal of the one user to the portable terminal of the
20 other user without being tampered with, the public key K_p is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key K_c based on a second generation algorithm, while the personal computer of the one
25 user generates the symmetric key K_c based on the second generation algorithm from information transmitted from the personal computer of the other user in cipher according to

the public key; and thereafter both the personal computers send and receive data in cipher according to the symmetric key Kc.

5 According to an ad-hoc radio communication data send/receive system and method of the present invention utilizing the
aforementioned ad-hoc radio communication verification
system, the system includes a portable terminal having a
radio communication function and a personal computer having
a radio communication function that are owned by each user,
10 wherein the portable terminal and personal computer of each user are connected by a secure communication path; when the ad-hoc radio communication verification system verifies that a public key Kp of one user is transmitted from the portable terminal of the one user to the portable terminal of the
15 other user without being tampered with, the portable terminal of the other user generates a symmetric key Kc based on a second generation algorithm, while the portable terminal of the one user generates the symmetric key Kc based on the second generation algorithm from information
20 transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key Kc is transmitted from the portable terminal to the personal computer of each user; and thereafter both the personal computers send and receive data in cipher according to the
25 symmetric key Kc.

According to an ad-hoc radio communication data send/receive system and method of the present invention, the system

includes a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key K_p of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the public key K_p is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key K_c based on a second generation algorithm, while the personal computer of the one user generates the symmetric key K_c based on the second generation algorithm from information transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the personal computers send and receive data in cipher according to the symmetric key K_c .

According to an ad-hoc radio communication data send/receive system and method of the present invention, the system includes a portable terminal having a radio communication function and a personal computer having a radio communication function that are owned by each user, wherein the portable terminal and personal computer of each user are connected by a secure communication path; when it is verified that a public key K_p of one user is transmitted from the portable terminal of the one user to the portable terminal of the other user without being tampered with, the

portable terminal of the other user generates a symmetric key Kc based on a second generation algorithm, while the portable terminal of the one user generates the symmetric key Kc based on the second generation algorithm from
5 information transmitted from the portable terminal of the other user in cipher according to the public key, then the symmetric key Kc is transmitted from the portable terminal to the personal computer of each user; thereafter both the personal computers send and receive data in cipher according
10 to the symmetric key Kc.

The secure communication path between a portable terminal having a radio communication function and a personal computer having a radio communication function of each user is established by mutual communication using a private key of each user, for example. A portable terminal having a
15 radio communication function includes so-called PDA (personal digital assistant). A hidden computing (described later) is considered as an example of style where a businessman works. For hidden computing, it is desirable
20 that personal computers having a radio communication function, such as a notebook computer, can mutually send and receive data without being tampered with. If it is verified that a public key Kp of one portable terminal having a radio communication function is transmitted to the other portable
25 terminal having a radio communication function without being tampered with on the way, as a result of the comparison between the verification data at the verification data output sections of portable terminals, the personal computers having a radio communication function of both

users take over that verification, thereafter the cipher communication can be smoothly performed between both the personal computers using the symmetric key Kc.

5 A program that is recorded or delivered by a recording media or a delivery system of the present invention comprises the steps of:

10 sending data for verification data generation from one data send/receive device to the other data send/receive device, wherein the two data send/receive devices are mutually connected by an ad-hoc radio connection; in the one data send/receive device, outputting verification data to its own verification data output section, wherein the verification data is generated based on a first generation algorithm from the sent data for verification data generation; in the
15 other data send/receive device, outputting verification data to its own verification data output section, wherein the verification data is generated based on the first generation algorithm from the received data for verification data generation; and determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually.
20

25 Further, it is characterized in that the verification data is visual or auditory verification data.

It is still further characterized in that the verification

data is output at the verification data output section both in the visual form and auditory form.

The program that is recorded or delivered by a recording media or a delivery system of the present invention further comprises the steps of:

defining a function as an operator, a numeric on which the operator operates as an input of the operator, and an operation result of the operator as an output of the operator; establishing a serial sequence of operators that are composed of one or more of operators arranged in series, wherein the operators relate to the same or different one-way functions; letting an input to the serial sequence of operators be data for verification data generation and an output from the serial sequence of operators or a corresponding value be verification data.

It is further characterized in that the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually.

Advantageous Embodiment

Now an example embodiment of the present invention will be described referring to the attached drawings.

Fig. 4 is a flowchart illustrating the verification of data integrity and subsequent cipher data transmission. A requester and the requested end of the establishment of cipher communication are defined as a source and destination respectively, wherein the source data send/receive device is shown as A, while the destination data send/receive device is shown as B in Fig. 4. The source and destination of a public key for verification of data integrity do not necessarily match the source and destination of a main transmission (i.e., cipher transmission using a symmetric key) after the verification of data integrity, so that the inverse relation may be allowed. Furthermore, during the main transmission, the source and destination may be properly changed.

Now, the procedure shown in Fig. 4 will be described in order.

(a) Source A sends to destination B its own public key K_p and an ID (hereinafter called "ID1") that specifies a verification data generation algorithm, along with a request for establishment of a cipher communication path. At the same time, source A generates verification data X_p based on its own public key K_p .

(b) Let data that destination B received from source A for a public key K_p be K_x . If there is no tampering of data on the radio communication path from source A to destination B, K_x equals K_p , while if there is tampering, K_x differs from K_p . Destination B generates verification data X_x based on K_x received from source A

using the generation algorithm corresponding to ID1 specified by source A. An example of verification data will be described referring to Fig. 5.

5 (c) Users of source A and destination B verify whether verification data X_p and X_x that are displayed in the respective displays are the same. If X_p equals X_x , this means K_x equals K_p , hence it is determined that data integrity is assured for the communication path between source A and destination B.

10 (d) Destination B encrypts the random number R for generating a symmetric key and an ID (hereinafter called "ID2") that specifies a symmetric key generation algorithm and sends them to source A. The transmission of ID2 between source A and destination B may be
15 omitted like ID1, if ID2 is fixed such as when source A and destination B use the same communication software. At the same time, destination B generates a symmetric key K_c using the symmetric key generation algorithm.

20 (e) Source A decodes a random number R received from destination B using a private key corresponding to the public key K_p to get the random number R and ID2, then generates a symmetric key K_c from the random number R using the symmetric key generation algorithm specified by ID2.

25 (f) Thereafter, source A and destination B send and receive data by means of cipher communication based on the symmetric key K_c .

Verification data displayed in the verification data output

sections of source A and destination B may be the data for verification data generation itself, for example, the public key of source A itself. That is, the public key of source A may be displayed in bits as the data for verification data generation. Alternatively, the numeric representation of the public key may be transformed into an image representation to facilitate the comprehension. Fig. 5 is a histogram showing an example of verification data generated from data for verification data generation. The verification data is displayed in the verification image display section 27 of the data send/receive device 20 (Fig. 10) . Assuming that the data for verification data generation is a public key of source A, and the public key is divided into a plurality of divisions having an equal number of bits in order, from MSB toward LSB, then the verification data is represented by the histogram, wherein the horizontal axis represents the divisions, while the vertical axis represents the quantity corresponding to each division. If the public key K_p of source A is not pretended by a malicious third party on the way of the transmission line, the data for verification data generation K_x that destination B received from source A equals the data for verification data generation K_p , i.e., $K_x = K_p$. Therefore, when a user of source A and destination B or any other reliable verifier directly watches the display section of source A or destination B and ascertains that X_p and X_x match each other as a result of comparison, he determines that the public key of source A was transmitted to destination B as it is, that is, the data integrity is

assured. On the other hand, when X_p and X_x do not match, it is determined that there was tampering of data on the way of transmission line from source A to destination B.

However, since the accuracy of recognition capability of human beings is not necessarily high, there may be a case where the difference from a similar public key having a small hamming distance could not be detected only by generating a comparative image, such as a histogram shown in Fig. 5. Therefore, it might be effective to apply a one-way function such as a hash function to the public key to transform into a predetermined data and display it as a verification image such as a histogram. In this case, even if a third party who tries to make a pretense seeks for another public key that outputs similar data, such an attempt is impossible in terms of calculated amount since he must solve a discrete logarithmic problem. However, information amount of the created verification image is extremely small compared with a bit size of a public key, it may be breached by a complete search. Under such conditions, it might be effective to apply a further one-way function to data that has already been applied a one-way function to calculate new data, or apply another one-way function to a public key to calculate new data, thereby generating a verification image. A plurality of verification images are generated by repeating this operation, as a result, the resistance to pretense is improved.

Verification data is not limited to an image such as a histogram, it may be a display of character data, a change of tonal scales, or a combination thereof. For auditory verification data, a vertical axis of the histogram of Fig. 5 corresponds to the pitch of sounds or the tone, while the horizontal axis represents sounds corresponding to a value of each division in order for every predetermined time. Further, the verification data may be output using both a visual display and an auditory speaker.

Fig. 6 through Fig. 8 show how to generate verification data from the data for verification data generation using a one-way function. Data D1 refers to data for verification data generation, while data D2, D3 and D4 refer to mean verification data. Each one-way function functions as an operator, which operates upon an input and outputs an operation result. A one-way function may be a hash function, for example.

In Fig. 6, a one-way function F is operated on data D1 to get data D2 at the first time, wherein D1 is data for verification data generation. At the second time, the same one-way function F is operated on data D2 to get data D3, that is, a loop including a one-way function F is formed. Thereafter, a loop processing is repeated to get data D4, D5, etc. After a predetermined number of repeats, a final operation result Dn is obtained, which is made the verification data and displayed in the verification image display section 27 of the data send/receive device 20 (see

Fig. 10). In addition to the final operation result Dn, some or all of operation results D2, D3, D4, etc., may be displayed in the verification image display section 27 of the data send/receive device 20 for comparison, utilizing screen separation or time division. By comparing a plurality of verification data, even if one of them is confusing to determine match or mismatch, it is very unlikely that all of them are confusing to determine match or mismatch, thereby improving the accuracy of verification in relation to data tampering.

When comparing not all of D2, D3, D4, etc., but only specific some of them, the protection against a malicious third party is improved by changing a subset of them properly.

In Fig. 7, a plurality of different one-way functions F, G, H, etc. are provided to operate on common data D1 to get each operation result D2, D3, D4, etc. Specific some or all of D2, D3, D4, etc., are displayed as verification data for comparison in the verification image display section 27 of the data send/receive device 20 by means of screen separation or time division.

In Fig. 8, a plurality of different one-way functions F, G, H, etc., are provided. At the first time, a one-way function F is operated on data D1 to get data D2, wherein D1 is data for verification data generation. At the second time, a one-way function G is operated on data D2 to get data D3. Like this, a subsequent one-way function is

operated on the previous operation result to get a plurality of D2, D3, D4, etc. Specific some or all of D2, D3, D4, etc., are displayed as verification data for comparison in the verification image display section 27 of the data
5 send/receive device 20 by means of screen separation or time division. It is noted that the method for comparing a plurality of verification data shown in Fig. 6 is regarded as a specific example of Fig. 8, where the same one-way function F is used in place of different one-way functions.

10 Fig. 9 is a block diagram showing a method for getting verification data by combining the processing of Fig. 6 through Fig. 8, wherein the operation type of verification data is defined as type 1, type 2 and type 3, respectively. The data for verification data generation is input to the
15 far left of Fig. 9, while the verification data is output from the far right of Fig. 9. An arrangement shown in Fig. 9 is no more than an example and the data for verification data generation is obtained by selecting two or more of types from type 1, 2 and 3 and arranging them in any order.

20 Fig. 10 is a block diagram of the data send/receive device 20. Since the data send/receive device 20 becomes source A or destination B according to circumstances, it provides for both configurations for source and destination at the same time. When the data send/receive device 20 is source A, the
25 transmission verify section 24 outputs its own public key to the verification image generate section 26, while when the data send/receive device 20 is source B, a public key of

source A, which is received at the communication section 25 as send/receive data 31 from source A, is sent to the verification image generate section 26 via the transmission verify section 24. The verification image generate section 26 generates verification data from the public key received from the transmission verify section 24, wherein the generated verification data is displayed in the verification image display section 27. A user of source A and destination B compares the verification data in the verification image display section 27 of two data send/receive devices 20 that are connected via ad-hoc radio connection to check match or mismatch, then inputs the result to the verification result input section 28. The input result is then informed to the transmission verify section 24, wherein the transmission verify section 24 determines that the public key transmitted from source A to destination B via the transmission line for ad-hoc radio connection is secured its data integrity when informed that both the verification data matches. Next, when the data send/receive device 20 is source B, a random number is generated in the random number generate section 34, then a symmetric key is generated from the random number based on the symmetric key generation algorithm of ID2 in the symmetric key generate section 33. On the other hand, the random number generated in the random number generate section 34 and ID2 are encrypted based on the public key of source A in the decode/encrypt section 32, then the cipher data Dc is transmitted to source A via the send/receive data 31. The symmetric key generated based on the symmetric key

generation algorithm of ID2 is stored in the key storage section 35. When the data send/receive device 20 is source A, the send/receive data 31 of cipher data Dc transmitted from destination B is decoded using own private key in the
5 decode/encrypt section 32 to get the random number R and ID2, then the symmetric key is generated from the random number R based on the symmetric key generation algorithm of ID2 and stored in the key storage section 35. Subsequently, when sending data, the symmetric key is retrieved from the
10 key storage section 35, then the send data is encrypted based on the symmetric key in the decode/encrypt section 32 and sent to the opponent as the send/receive data 31. When receiving data, the encrypted send/received data 31 received is decoded in the decode/encrypt section 32, then the plain
15 data may be stored in a hard disk (not shown) or a predetermined processing may be performed.

Fig. 11 is a flowchart of communication processing on the side of source A. First, it sends a public key Kp (step 40), then generates verification data Xp from the public key Kp based on the verification data generation algorithm of ID1 (step 42), and displays the verification data Xp in the
20 verification image display section 27 (step 44). In step 46, own verification data Xp is compared with verification data Xx of destination B, as a result, if the comparison matches, the process proceeds to step 48, while mismatches, the process is terminated for error (i.e., data integrity is not secured). If data integrity is secured, the process
25 waits for receipt of the random number R from destination B

(step 48). If it is determined that the random number R is received in step 50, the process proceeds to step 52, while the process is terminated when the random number R has not been received despite a predetermined time has passed. In step 52, cipher data of the random number R from the destination B is decoded using own private key corresponding the public key Kp to get the random number R. It should be noted that between the data send/receive devices A and B, an ID is arranged in advance for each of a plurality of symmetric key generation algorithms, wherein an ID (e.g., ID2 in this example) that was employed at destination B as a symmetric key generation algorithm is transmitted to source A from destination B along with the random number R. In step 56, a symmetric key for communication with destination B is generated from the random number R based on a symmetric key generation algorithm of ID2, thereafter, cipher communication starts with destination B using the symmetric key (step 58).

Fig. 12 is a flowchart of communication processing on the side of destination B. First, it receives a public key Kx (step 60). Note that this received public key is referred to as Kx rather than Kc here, because it might be tampered with by a malicious third party intervening on the transmission line between source A and destination B. Next, verification data Xx is generated from Kx based on the verification data generation algorithm specified by ID1 that was sent from source A with a public key Kp (step 62), then the verification data Xx is output to the verification image

display section 27 (step 64). In step 66, own verification data Xx is compared with verification data Xp of source A, as a result, if the comparison matches, the process proceeds to step 68, while mismatches, the process is terminated for error (i.e., data integrity is not secured). If data integrity is secured, a random number R is generated (step 68), then the random number R and ID2, which is the ID of a symmetric key generation algorithm selected among a plurality of symmetric key generation algorithms this time, are encrypted using a public key of source A and transmitted to source A (step 70), then the symmetric key Kc is generated based on the symmetric key generation algorithm of ID2 (step 72), thereafter, cipher communication starts with source A using the symmetric key (step 74).

Fig. 13 is a diagram for illustrating how to establish a cipher communication path for an ad-hoc radio connection between users who utilize a hidden computing style. The hidden computing means the utilization style where a user puts a computer in a bag and operates it by remote control using a radio communication from a portable device such as PDA (personal digital assistant) on hand. A reference number 82 is a communication device that is equipped in the PDA 80a. When performing ad-hoc radio communication between the devices (i.e., notebook computers 88a and 88b in bags 86a and 86b, respectively) which are not equipped with a system that can verify the data integrity of a public key as described above, a cipher communication path is established indirectly using PDAs 80a and 80b, which maintain secure

communication paths 90a and 90b in advance with notebook computers 88a and 88b that mount a cipher communication path establishment protocol. A secure communication path between a PDA and a notebook computer is established by means of, 5 for example, cipher communication using a symmetric key that is arranged in advance between both parties. In Fig. 13, first in the procedure (a), a communication path 84 is established between PDA 80a and PDA 80b, then a public key of one PDA is transmitted to the other PDA to verify data 10 integrity of the public key. Next, in the procedure (b), verification of data integrity between PDA 80a and PDA 80b is inherited to the notebook computers 88a and 88b, which are connected with PDAs 80a and 80b respectively by means of a secure communication paths 90a and 90b. Specifically, 15 this inheritance is achieved by transmitting a public key, which is verified of its data integrity between PDAs 80a and 80b, to notebook computers 88a and 88b via secure communication paths 90a and 90b. Thereafter, notebook computers 88a and 88b share a symmetric key via 20 communication path 92, then send and receive data in cipher according to the symmetric key.

The present invention can be realized in hardware, software, or a combination of hardware and software. The present invention can be realized in a centralized fashion in one 25 computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system - or other apparatus adapted for carrying out the methods described herein - is

suitable. A typical combination of hardware and software could be a general purpose computer system with a computer program that, when being loaded and executed, controls the computer system such that it carries out the methods described herein. The present invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which - when loaded in a computer system - is able to carry out these methods.

Computer program means or computer program in the present context mean any expression, in any language, code or notation, of a set of instructions intended to cause a system having an information processing capability to perform a particular function either directly or after conversion to another language, code or notation and/or reproduction in a different material form.

It is noted that the foregoing has outlined some of the more pertinent objects and embodiments of the present invention. This invention may be used for many applications. Thus, although the description is made for particular arrangements and methods, the intent and concept of the invention is suitable and applicable to other arrangements and applications. It will be clear to those skilled in the art that other modifications to the disclosed embodiments can be effected without departing from the spirit and scope of the invention. The described embodiments ought to be construed to be merely illustrative of some of the more prominent

features and applications of the invention. Other beneficial results can be realized by applying the disclosed invention in a different manner or modifying the invention in ways known to those familiar with the art.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233